INTERNATIONAL STANDARD

ISO/IEC 15026-4

First edition
2012-10-01

Systems and software engineering — Systems and software assurance —

Part 4: Assurance in the life cycle

Ingénierie du logiciel et des systèmes — Assurance du logiciel et des systèmes —

Partie 4: Assurance du cycle de vie

Reference number
ISO/IEC 15026-4:2012(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 15026-4 was prepared by Joint Technical Committee ISO/TC JTC 1, *Information technology*, Subcommittee SC 7, *Software and systems engineering*.

ISO/IEC 15026 consists of the following parts, under the general title *Systems and software engineering — Systems and software assurance*:

— *Part 1: Concepts and vocabulary* [Technical Report]

— *Part 2: Assurance case*

— *Part 3: System integrity levels*

— *Part 4: Assurance in the life cycle*

Introduction

In its entirety, ISO/IEC 15026 consists of multiple parts:

a) ISO/IEC TR 15026-1, *System and software engineering — Systems and software assurance — Part 1: Concepts and vocabulary*

NOTE ISO/IEC TR 15026-1 is intended to be replaced by an International Standard.

b) ISO/IEC 15026-2, *System and software engineering — Systems and software assurance — Part 2: Assurance case*

c) ISO/IEC 15026-3, *System and software engineering — Systems and software assurance — Part 3: System integrity levels*

d) ISO/IEC 15026-4, *System and software engineering — Systems and software assurance — Part 4: Assurance in the life cycle*

Many specialized standards and guidelines address specific application areas and topics related to assurance and use different concepts and terminology when addressing common themes. ISO/IEC TR 15026-1 provides terminology and concepts used in all parts of ISO/IEC 15026.

ISO/IEC 15026-2 provides minimum requirements for the structure and contents of assurance cases that treat claims regarding properties of a system or software product selected for special treatment. The results of performing the life cycle activities and tasks referenced in this part of ISO/IEC 15026 can be recorded in the form of the assurance case described in ISO/IEC 15026-2.

ISO/IEC 15026-3 addresses the assignment of integrity levels for selected elements of a system. Where ISO/IEC 15026-2 is applicable, it can bring useful structure, aid, and direction to defining claims and showing their achievement through the use of integrity levels and accompanying integrity level requirements.

ISO/IEC 15026-2, ISO/IEC 15026-3 and ISO/IEC 15026-4 all use the concepts and vocabulary defined in ISO/IEC TR 15026-1; however, any part can be applied independently of the others and the use of one does not require the use of any others.

Systems and software engineering — Systems and software assurance —

Part 4: Assurance in the life cycle

1 Scope

This part of ISO/IEC 15026 gives guidance and recommendations for conducting selected processes, activities and tasks for systems and software products requiring assurance claims for properties selected for special attention, called critical properties. This part of ISO/IEC 15026 specifies a property-independent list of processes, activities and tasks to achieve the claim and show the achievement of the claim. This part of ISO/IEC 15026 establishes the processes, activities, tasks, guidance and recommendations in the context of a defined life cycle model and set of life cycle processes for system and/or software life cycle management.

NOTE The stakeholders determine which of the system or software properties are selected for special attention and require assurance claims. This part of ISO/IEC 15026 uses the term “critical” to distinguish those properties from other requirements.

2 Conformance

Conformance may be claimed to this part of ISO/IEC 15026 with respect to the systems assurance process view and/or the software assurance process view. Thus, conformance to this part of ISO/IEC 15026 can be achieved in either or both of the following ways:

a) Demonstrating that the required outcomes of the systems assurance process view (6.1.2) have been achieved, in addition to conforming to the Agreement, Project, and Technical processes of ISO/IEC 15288.

b) Demonstrating that the required outcomes of the software assurance process view (6.2.2) have been achieved, in addition to conforming to the Agreement, Project, Technical, and Software Specific processes of ISO/IEC 12207:2008.

A claim of conformance is relevant only to specific claims regarding designated systems or software.

Conformance to ISO/IEC 15026 Part 2 can assist in achieving the outcomes required by the two process views in this part of ISO/IEC 15026.

NOTE Parties to an agreement may choose to incorporate selected portions of this part of the International Standard into the terms of the agreement. However, compliance with the agreement does not justify a claim of conformance to this part of the International Standard. A claim of conformance can only be justified as explained above.

3 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced documents (including any amendments) applies.

ISO/IEC TR 15026-1, *Systems and software engineering — Systems and software assurance — Part 1: Concepts and vocabulary*

This part requires activities and tasks in the context of complete sets of life cycle processes that comprise life cycle models for projects. The two sets of life cycle processes are provided in:

ISO/IEC 15288:2008, *Systems and software engineering — System life cycle processes*

ISO/IEC 12207:2008, *Systems and software engineering — Software life cycle processes*

The assurance guidance and recommendations referenced in this part of ISO/IEC 15026 are to be understood in terms of their being in the context of the processes, activities and tasks of ISO/IEC 15288 and ISO/IEC 12207.

4 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC TR 15026-1, ISO/IEC 15288:2008, and ISO/IEC 12207:2008 apply.

5 Key concepts for and use of this part of ISO/IEC 15026

5.1 Life cycle approach

It is presumed that the user of this International Standard is using a defined life cycle model and set of life cycle processes for system and/or software life cycle management. Across the life cycle, the systems and software process views in Clause 6 use the guidance and recommendations in Clause 7 for the performance of specific processes, activities, and tasks in order to achieve and show the achievement of assurance claims. Since all processes of ISO/IEC 15288 and ISO/IEC 12207 are applied iteratively and recursively in the life cycle, the guidance and recommendations for assurance are also applied iteratively and recursively. In that way, the achievement of assurance can be checked during each iteration or recursion.

NOTE See ISO/IEC TR 24748-1 for more information about life cycle models and the iteration and recursion of processes.

5.2 Assurance claims

When system or software product requirements call for assurance of one or more critical properties of the system or software product, the overall claims for assurance regarding these properties' values are referred to in ISO/IEC 15026 as assurance claims. Commonly, such critical properties are in areas where substantial risk or consequences are involved such as reliability and maintainability, safety, security, or human factors.

NOTE The material in this clause is adopted from ISO/IEC 15026-2.

Achieving assurance claims normally includes all the considerations involved in achieving stringent requirements. A requirement is defined in ISO/IEC 29148 as “statement which translates or expresses a need and its associated constraints and conditions” and a claim is defined in ISO/IEC TR 15026-1 as “statement of something to be true including associated conditions and limitations.” This part of ISO/IEC 15026 considers requirements to be statements of values for variables and claims to be statements of requirements to be true.

While assurance claims can be derived from a number of sources, they are normally motivated by potential real-world adverse consequences related to the intended uses of the system and justified as deriving from system or software requirements. Each assurance claim is fully and unambiguously specified including:

a) “Assurance claims” — that is, the top-level claims, including

   1) Values for the variables of the critical property required for its achievement.

   2) Limitations on allowable uncertainties regarding this achievement.

   3) Conditions and/or durations of applicability under which it applies.

4) The set of versions or instances of the system or software product covered by the claims.

c) “Justification for assurance claims” — that is, the justification for selecting and specifying these particular assurance claims.

d) “Body of information showing achievement of assurance claims” or more succinctly as the “information showing [or assuring] the achievement of assurance claims”.

This last item includes the evidence, the rationale or argument showing how the evidence supports the claims, and any assumptions underlying this rationale. Normally, this rationale has multiple levels of derived claims internal to it, e.g., claims about system elements at each level of decomposition that need to be true in order for the assurance claims about the system or software product to be true. The body of information also includes information on the validity, integrity, relevance, and significance of the evidence.

The rationale often includes several different kinds of arguments, e.g., arguments based on design rationale, use of defensive design techniques, verification and validation results, performance of similar systems or products, conformance to standards, or field data. These are combined to achieve an overall conclusion and an estimate of the remaining uncertainty regarding the achievement of the assurance claims.

The body of information composing and organizing these three items is an element (or elements) of the system or software product and, as such, is maintained and updated throughout the system life cycle, to include development as well as maintenance. As a system element, all the processes, activities, and tasks regarding a system element apply to it, such as configuration management, verification, and validation.

5.3 Using this part of ISO/IEC 15026

This part of ISO/IEC 15026 can be used for an agreement between an acquirer and supplier, for regulation purposes, or for assessment of internal development processes to improve achieving and showing the achievement of assurance claims for the system or software product. Its use is, however, not limited to these three purposes.

5.3.1 Use for an agreement

This part of ISO/IEC 15026 can be used for an agreement between an acquirer and a supplier concerning achieving and showing the achievement of an assurance claim about the value of variables for a critical property of the system or software product being acquired. The acquirer and supplier relationship can occur at different levels of the supply chain (prime-supplier, internal to one organization, etc.).

NOTE An agreement may range in formality from a written contract to a verbal understanding.

5.3.2 Use for regulation

An authoritative body can use this part of ISO/IEC 15026 for regulation for assuring some critical property of a system or software product. The need for such regulation can arise to assure or certify a critical property of a system or software product, to clarify their assurance in the condition of trade, or to do some other action.

5.3.3 Use for development

This part of ISO/IEC 15026 can be used for an internal assessment by a developer in improving its processes for achieving and showing the achievement of assurance claims for critical properties of systems and software products it develops.

6 Process view purposes and required outcomes

6.1 Systems assurance process view

The following clauses define the purpose and required outcomes of the systems assurance process view.

6.1.1 Purpose

The purpose of the Systems Assurance Process View is to achieve the assurance claims regarding the system properties selected for special attention and to provide a body of information showing the achievement of those claims. The Systems Assurance Process View covers the system of interest including any constituent software.

6.1.2 Required outcomes

The following outcomes shall result from the successful implementation of the Systems Assurance Process View:

a) A subset of requirements for the achievement of critical properties is defined.

b) Assurance claims, their justification, and the body of information showing the achievement of the assurance claims for the critical properties are established as an element of the system.

c) A strategy for achieving these assurance claims and showing their achievement is defined.

d) The extent of achievement of the assurance claims is communicated to affected stakeholders.

6.2 Software assurance process view

The following clauses define the purpose and required outcomes of the software assurance process view.

6.2.1 Purpose

The purpose of the Software Assurance Process View is to achieve the assurance claims regarding the software properties selected for special attention and to provide a body of information showing the achievement of those claims.

6.2.2 Required outcomes

The following outcomes shall result from the successful implementation of the Software Assurance Process View:

a) A subset of requirements for achievement of the critical properties for application of this process view is defined.

b) Assurance claims, their justification, and the body of information showing achievement of the assurance claims for the critical properties are established as an element of the system.

c) A strategy for achieving these assurance claims and showing their achievement is defined.

d) The extent of achievement of the assurance claims is communicated to affected stakeholders.

7 Assurance guidance and recommendations for selected processes

7.1 Introduction

Clause 7 cites the activities and tasks from the Agreement, Project, and Technical categories of processes in ISO/IEC 15288:2008 and in ISO/IEC 12207:2008 that require extension or special interpretation when a defined level of assurance is to be demonstrated. The numbers of those activities and tasks correspond to the numbers in the parent standards (ISO/IEC 15288 and ISO/IEC 12207). Assurance-claim-related guidance and recommendations are provided for performing these activities and tasks to achieve the outcomes of the process views. This guidance and recommendations assume and depend upon the full application of ISO/IEC 15288 and ISO/IEC 12207 as indicated in Clause 3. The processes and activities not cited in this clause are considered adequate as defined in ISO/IEC 15288:2008 and ISO/IEC 12207:2008 to achieve the claims for the critical properties.

7.2 Acquisition process

The Acquisition Process (ISO/IEC 15288:2008, 6.1.1 and ISO/IEC 12207:2008 6.1.1) obtains a product or service in accordance with the acquirer's requirements. When the acquisition is for a system element, this process should ensure that all requirements for achieving or showing the achievement of any assurance claim associated with that system element is passed to the supplier through the agreement.

7.2.1 Relevant activities and tasks

Activities from 15288	Activities from 12207
6.1.1.3 c) Initiate an agreement. 1) Negotiate an agreement with the supplier. d) Monitor the agreement. 1) Assess the execution of the agreement. 2) Provide data needed by the supplier and resolve issues in a timely manner.	6.1.1.3.4 Contract agreement. 6.1.1.3.4.2 The acquirer shall then prepare and negotiate an agreement with the supplier that addresses the acquisition requirements, including the cost and schedule, of the software product or service to be delivered. The contract shall address proprietary, usage, ownership, warranty and licensing rights associated with the reusable off-the-shelf software products. 6.1.1.3.5 Agreement monitoring. 6.1.1.3.5.1 The acquirer shall monitor the supplier's activities in accordance with the Software Review Process and the Software Audit Process. The acquirer should supplement the monitoring with the Software Verification Process and the Software Validation Process as needed.

7.2.2 Assurance guidance and recommendations

The project should ensure that the agreement considers the variables and their values of the critical properties for the system element being acquired. The agreement should include integrity requirements (i.e., guarding against counterfeit parts, tampering, system elements with vulnerabilities, and revealing of confidential information including information about vulnerabilities to ensure that what is received is what is expected. The project should derive the claims for the system element being acquired from the system's assurance claims and incorporate them into the request for the supply of the system element. In addition, the project should incorporate the following considerations into the negotiations and the agreement with the supplier:

a) Confidence that the appropriate controls regarding dependability (e.g., trustworthiness) of their personnel and those of their associated organizations are effectively implemented.

b) Confidence that the supplier guards against counterfeit parts, tampering, and other threats to system or product integrity as well as against revealing confidential information.

c) Confidence that the system element transferred, received, and, to the extent practicable, installed and operated, is the one intended.

d) Confidence that the product development environment has appropriate resources in place to protect the integrity of the product and its critical properties during development.

e) Confidence that the system or software development life cycle model chosen by the supplier is appropriate to the nature of any assurance claims to be achieved.

f) Confidence that the appropriate controls regarding implementation of dependability and safety requirements and the achievement of system dependability and safety integrity requirements are effectively implemented.

g) Confidence that the development lifecycle is conducted using well documented, repeatable processes that are monitored in accordance with a quality management plan appropriate to the nature of the claims to be achieved.

The project should revisit the approaches to showing achievement of claims when considering an acquisition from a supplier when the supplier relationship changes (i.e. new, acquired by another entity, merged with another entity) or if the acquirer's requirements change to ensure that the supplier does not deny required information, enable a new threat, or undermine the safeguards already in place to protect the system.

The project should submit a request for proposal (RFP) that can be correctly understood by the supplier and other stakeholders and establish a procedure for resolving problems, which may even expand to a change in the agreement in the case of extensive problem resolution. Upon a change of agreement, the project should ensure that the stakeholder requirements defined in the Stakeholder Requirements Definition process are the starting point of the change. The project should consider a multi-stage agreement when appropriate.

NOTE Refer to ISO/IEC 12207:2008 Annex F.3 of for a description of the Contract change management process.

7.3 Supply process

The Supply Process (ISO/IEC 15288:2008, 6.1.2 and ISO/IEC 12207:2008 6.1.2) provides an acquirer with a product or service that meets agreed requirements. When a system element is being supplied, this process should ensure that all requirements for achieving or showing the achievement of any assurance claim associated with that system element are passed to the acquirer.

7.3.1 Relevant activities and tasks

Systems Assurance Process View	Software Assurance Process View
6.1.2.3 c) Initiate an agreement 1) Negotiate an agreement with the acquirer. d) Execute the agreement. 1) Execute the agreement according to the Supplier's established project plans and in accordance with the agreement. 2) Assess the execution of the agreement.	6.1.2.3.4 Contract execution. 6.1.2.3.4.8 The supplier shall monitor and control the progress and the quality of the software products or services of the project throughout the contracted life cycle. This shall be an ongoing, iterative task, which shall provide for: a) Monitoring progress of technical performance, costs, and schedules and reporting of project status. b) Problem identification, recording, analysis, and resolution.

7.3.2 Assurance guidance and recommendations

The project should ensure that the agreement considers the feasibility of the variables and their values of the critical properties for the system element being supplied, from the technical and resources aspects. The agreement should include integrity requirements to ensure that what is supplied is what is expected. The project should provide the evidence and argument for the claims for the system element derived from the system's assurance claims. In addition, the project should incorporate the following considerations into the negotiations and the agreement with the acquirer, in order to achieve assurance which offsets the resource available to the project:

a) Confidence that there is a means to fulfil major requirements in a practical manner from technical and other aspects.

b) Consideration of a multistage agreement, in the case that the precise cost estimation is difficult to achieve.

c) Consideration of stepwise commencement of operations of the system, should there be a possibility of missing the deadline due to unexpected reason.